A publication of the DCIS Northeast Field Office

TECHNOBABBLE

The DCIS Cyber Crime Newsletter

TECHNOBABBLE
Volume 3, Issue 1

January, 2002

This issues suggested computer crime bookmarks:

Software & Information Industry Association:
http://www.siia.net

Business Software Alliance:
http://www.bsa.org

Emory University's 'Software Piracy & the Law' Site :
http://www.emory.edu/ITD/POLICY/bsa.html

Inside this issue:

Federal Law Enforcement Battles Software Piracy

On December 11, 2001, Attorney General John Ashcroft announced that in three separate federal law enforcement actions federal agents executed approximately 100 search warrants worldwide against virtually every level of criminal organizations engaged in illegal software piracy over the Internet. The three Operations, codenamed "Buccaneer," "Bandwidth" and "Digital Piratez," struck at all aspects of the illegal software, game and movie trade, often referred to as "warez scene."

"Today U.S. law enforcement initiated the most aggressive enforcement action to date against illegal software piracy," Attorney General Ashcroft said. "Many of these individuals and groups believed the digital age and the Internet allowed them to operate without fear of detection or criminal sanction. Today, law enforcement in the U.S. and around the world proved them wrong. These actions mark a significant milestone in the efforts of U.S. law enforcement to work internationally to combat what is truly a global problem," said Ashcroft.

"The execution of these search warrants mark the completion of the most extensive software piracy undercover investigation that the FBI has participated in to date, and should send the message that trafficking in stolen goods – whether the property is in physical or electronic form – is a serious crime, and will be prosecuted," said Robert S. Mueller, Director of the Federal Bureau of Investigation.

The targets of these Operations included both individuals and organizations, known as "WAREZ" groups, that operate within the United States and in various nations around the world and specialize in the illegal distribution over the Internet of copyrighted software programs, computer games and movies. The investigations will continue to identify and pursue additional targets in the months ahead.

Operation Buccaneer:

Operation Buccaneer was the culmination of an investigation that has been ongoing for over a year under the direction of the U.S. Customs Service and the Justice Department's Computer Crime and Intellectual Property Section, working in conjunction with the U.S. Attorney for the Eastern District of Virginia.

Buccaneer marks the most significant law enforcement penetration ever of international organizations engaged in the illegal distribution of copyrighted software, games and movies over the Internet. The enforcement action involved the simultaneous execution of 58 search warrants against high-level warez leadership and members within the United States and abroad. It is also the first enforcement action to reach across international borders and strike at the most highly placed and skilled members of these international criminal enterprises.

Although one of the primary criminal enterprises targeted by Operation Buccaneer was the warez group known as "DrinkOrDie," which consists of approximately 40 members worldwide, the investigation has led to infiltration and development of cases against individuals from other top groups as well.

The organizations targeted by Buccaneer are highly structured and security-conscious criminal groups that specialize in obtaining the latest computer software,

Federal Law Enforcement Battles Software Piracy

(Continued from Page 1)

games, and movies; stripping ("cracking") copyright protections; and releasing the final product to hundreds of Internet sites worldwide. Because the "suppliers" to these groups are often company insiders, pirated products frequently are in circulation before, or within hours, of the release of the legitimate product to consumers. The groups are structured specifically to avoid detection. It is expected that hundreds of thousands of copies of software programs, computer games and movies will be recovered by this effort, with a retail value that is expected to be in the millions of dollars.

Buccaneer also marks an unprecedented degree of cooperation and coordination with international law enforcement in the fight against Intellectual Property violations committed via the Internet. Through a variety of authorized means, the United States has shared evidence with counterparts in the United Kingdom, Australia, Norway, and Finland to help further identify and investigate numerous significant foreign targets engaged in this criminal conspiracy.

Operation Bandwidth:

On December 11, 2001, the longest-running of the undercover operations culminated with the execution of over 30 search warrants across the United States and Canada. This undercover operation, code-named 'Bandwidth,' was a two-year covert investigation established as a joint investigative effort to gather evidence to support identification and prosecution of entities and individuals involved with illegal access to computer systems and the piracy of proprietary software utilizing 'warez' storage sites on the Internet.

Bandwidth, through the joint efforts of the Defense Criminal Investigative Service (DCIS), the Environmental Protection Agency Office of Inspector General (EPA-OIG), and the Federal Bureau of Investigation (FBI), supervised by the U.S. Attorney's Office for the District of Nevada, created a 'warez' site, controlled and monitored by the undercover operation, as a means of attracting predicated targets involved with the distribution of pirated software. The undercover 'warez' site has been accessed to transfer over 100,000 files, including over 12,000 separate software programs, movies and games.

Over 200 different individuals participated in the software pirating efforts. Those individuals were able to attain first-run movies, the latest computer games, and versions of notable software products even before they were publicly introduced. As a result of Operation Bandwidth, thousands of copies of pirated software are expected to be removed from circulation, as well as the seizure and forfeiture of the computer hardware and servers used to facilitate the crimes.

Operation Digital Piratez:

Operation Digital Piratez is a year-long undercover operation by the Federal Bureau of Investigation's Boston Field Office, which has been supervised by the United States Attorney's Office for the District of New Hampshire. On December 11, 2001, the FBI executed nine search warrant, and obtained consent for an additional three searches, on computers located across the country. During this investigation, undercover Special Agents of the Federal Bureau of Investigation successfully infiltrated several Warez distribution organizations. This investigation targeted not only the Warez sites and those who operated them, it also targeted the "cracking groups" specifically created for the purpose of pirating software so that it may be distributed over the Internet in violation old U.S. copyright laws.

Each of the ongoing investigations has benefited from the important assistance provided by various intellectual property trade associations, including the Interactive Digital Software Association, the Business Software Alliance, the Motion Picture Association and individual companies, including Microsoft and Sega Corporation.

"Today U.S. law enforcement initiated the most aggressive enforcement action to date against illegal software piracy," Attorney General Ashcroft said. "Many of these individuals and groups believed the digital age and the Internet allowed them to operate without fear of detection or criminal sanction. Today, law enforcement in the U.S. and around the world proved them wrong. These actions mark a significant milestone in the efforts of U.S. law enforcement to work internationally to combat what is truly a global problem,"

Know the Code!

Common Federal Statutes Utilized in Prosecuting Computer Crime
By Special Agent Jim Ives, DCIS Boston Resident Agency

18 USC 2511 – Interception and Disclosure of Wire, Oral, or Electronic Communications

This issues 'commonly utilized statute' is 18 USC 2511, entitled "Interception and Disclosure of Wire, Oral, or Electronic Communications." The statute is of special significance to investigations which uncover the illegal use of sniffers and similar data gathering tools.

In part, the statute consists of the following language:

"In recent years, prosecutors have found that the statutes' focus upon wire, cable, and radio wave based transmissions has made the law quite applicable to Internet and intranet based crimes involving the illicit capture of data."

(1) Except as otherwise specifically provided in this chapter any person who–

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when--

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(e) (i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b) to (c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation, shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

The statute continues by defining various exceptions to violations, including approved law enforcement monitoring, etc., and defines various penalties for violating the statute (generally punishable by up to 5 years imprisonment, and various fines).

18 USC 2511 is yet another statute which was created for one purpose, yet lends itself to prosecution of computer crimes via its' open-ended wording. The statute was originally designed to punish individuals who illegally monitor and/or capture

Know the Code!

(Continued from Page 3)

transmissions which traverse wires or airwaves. Throughout history, the statute has been especially useful in prosecuting individuals or entities that establish illegal telephone wiretaps, or listening devices which capture radio wave communications. Examples of cases prosecuted by the government through utilization of this statute include instances whereby organized crime groups illegally wiretapped various individuals, cases whereby corporations established illegal listening devices in order to steal proprietary or sensitive competitive information, and cases whereby overly aggressive law enforcement officers utilized wiretaps without obtaining appropriate court authority.

In recent years, prosecutors have found that the statutes' focus upon wire, cable, and radio wave based transmissions has made the law quite applicable to Internet and intranet based crimes involving the illicit capture of data. Since any network based crime involves transmissions which traverse wire (as in cases involving dial-up access), cable (as in cases involving cable based Internet access), or airwaves (as in cases involving wireless Ethernet communications, or wireless Internet access), the statute lends itself nicely to computer based crime investigations, assuming some portion of data streams is captured. Once again, the nature of computer crime ensures that a large majority of investigations will uncover such occurrences. Most serious computer criminals have the goal of capturing data of relevance, such as financial data or intellectual property which can be used to their advantage. Even less nefarious computer criminals (i.e. so called "white hat" hackers who claim to compromise systems merely for the thrill of such activities, and who eventually broadcast security vulnerabilities to systems administrators without undertaking truly destructive behavior) are oftentimes guilty of violating 18 USC 2511. For example, such an intruder may utilize automated vulnerability assessment tools which briefly capture TCP/IP sessions containing a password/ user name in order to initially access a system. While utilization of such a tactic is not likely to seriously impact a system, it would, in theory, violate 18 USC 2511, and the individual could be prosecuted under the statute.

TRICARE Employee Pleas to Child Porn Charges

On December 14, 2001, the Defense Criminal Investigative Service (DCIS), Mid-Atlantic Field Office announced that Chris Eugene Wiley of Centreville, VA, waived indictment and pled guilty to a single count of criminal information for possession of child pornography.

Wiley, a health systems specialist for the TRICARE Management Activity (TMA), Falls Church, VA, entered his plea before U.S. District Court Judge Claude M. Hilton, Eastern District of Virginia, and is scheduled for sentencing on March 8, 2002.

TRICARE (formerly known as CHAMPUS) is the U.S. Department of Defense (DoD) component which supplies health care coverage to retired U.S. military personnel and military dependents.

The criminal information alleges Wiley did unlawfully and knowingly possess computer disks and other material that contained images of child pornography. The criminal information is the result of an investigation into allegations Wiley downloaded and viewed child pornography while using his Department of Defense computer at the TMA.

Wiley faces up to 5 years imprisonment, a fine of $250,000, full restitution, a special assessment and 3 years of supervised release.

The investigation was prosecuted by the U.S. Attorneys Office, Eastern District of Virginia.

'U.S. Patriot Act' Impacts Cyber Crime Investigations

In response to the tragic events of September 11, 2001, President Bush signed the U.S. Patriot Act into law on October 26, 2001. While the act was primarily designed to increase federal law enforcement's abilities to investigate and prosecute terrorist organizations operating within the United States, the act also implemented sweeping changes which impact computer crime related investigations.

The following (extracted from a U.S. Department of Justice White Paper which analyzes the act) refer to but a few computer crime related changes implemented as a result of the enactment of the U.S. Patriot Act:

Section 210 - Scope of subpoenas for Electronic Evidence

Previous law: Subsection 2703(c) allows the government to use a subpoena to compel a limited class of information, such as the customer's name, address, length of service, and means of payment. Prior to the amendments in Section 210 of the Act, however, the list of records that investigators could obtain with a subpoena did not include certain records (such as credit card number or other form of payment for the communication service) relevant to determining a customer's true identity. In many cases, users register with Internet service providers using false names. In order to hold these individuals responsible for criminal acts committed online, the method of payment is an essential means of determining true identity. Moreover, many of the definitions in section 2703(c) were technology-specific, relating primarily to telephone communications. For example, the list included "local and long distance telephone toll billing records," but did not include parallel terms for communications on computer networks, such as "records of session times and durations." Similarly, the previous list allowed the government to use a subpoena to obtain the customer's "telephone number or other subscriber number or identity," but did not define what that phrase meant in the context of Internet communications.

Amendment: Amendments to section 2703 (c) update and expand the narrow list of records that law enforcement authorities may obtain with a subpoena. The new subsection 2703(c)(2) includes "records of session times and durations," as well as "any temporarily assigned network address." In the Internet context, such records include the Internet Protocol (IP) address assigned by the provider to the customer or subscriber for a particular session, as well as the remote IP address from which a customer connects to the provider. Obtaining such records will make the process of identifying computer criminals and tracing their Internet communications faster and easier.

Section 211 - Clarifying the Scope of the Cable Act

Previous law: The law contains two different sets of rules regarding privacy protection of communications and their disclosure to law enforcement: one governing cable service (the "Cable Act") (47 U.S.C. § 551), and the other applying to the use of telephone service and Internet access (the wiretap statute, 18 U.S.C. § 2510 et seq.; ECPA, 18 U.S.C. § 2701 et seq.; and the pen register and trap and trace statute (the "pen/trap" statute), 18 U.S.C. § 3121 et seq.).

Amendment: Section 211 of the Act amends title 47, section 551(c)(2)(D), to clarify that ECPA, the wiretap statute, and the trap and trace statute govern disclosures by cable companies that relate to the provision of communication services – such as telephone and Internet services. The amendment preserves, however, the Cable Act's primacy with respect to records revealing what ordinary cable television programming a customer chooses to purchase, such as particular premium channels or "pay per view" shows. Thus, in a case where a customer receives both Internet access and conventional cable television service from a single cable provider, a government entity can use legal process under ECPA to compel the provider to disclose only those customer records relating to Internet service. (This section is not subject to the sunset provision in Section 224 of the Act).

Section 217- Intercepting the Communications of Computer Trespassers

Prior law: Although the wiretap statute allows computer owners to monitor the activity on their machines to protect their rights and property, until Section 217 of the Act was enacted it was unclear whether computer owners could obtain the assistance of law enforcement in conducting such monitoring. This lack of clarity prevented law enforcement from assisting victims to take the natural and reasonable steps in their own defense that would be entirely legal in the physical world. In the physical world, burglary victims may invite the police into their homes to help them catch burglars in the act of committing their crimes. The wiretap statute should not block investigators from responding to similar requests in the computer context simply because the means of committing the burglary happen to fall within the definition of a "wire or electronic communication" according to the wiretap statute. Indeed, because providers often lack the expertise, equipment, or financial resources required to monitor attacks themselves, they commonly have no effective way to exercise their rights to protect themselves from unauthorized attackers. This anomaly in the law created, as one commentator has noted, a "bizarre result," in which a "computer hacker's undeserved statutory privacy right trumps the legitimate privacy rights of the hacker's victims." Orin S. Kerr, *Are We Overprotecting Code? Thoughts on First-Generation Internet Law*, 57 Wash. & Lee L. Rev. 1287, 1300 (2000).

Amendment: To correct this problem, the amendments in Section 217 of the Act allow victims of computer attacks to authorize persons "acting under color of law" to monitor trespassers on their computer systems. Under new section 2511(2)(i), law enforcement may intercept the communications of a computer trespasser transmitted to, through, or from a protected computer. Before monitoring can occur, however, four requirements must be met. First, section 2511(2)(i)(I) requires that the owner or operator of the protected computer must authorize the interception of the trespasser's communications. Second, section 2511(2)(i)(II) requires that the person who intercepts the communication be lawfully engaged in an ongoing investigation. Both criminal and intelligence investigations qualify, but the authority to intercept ceases at the conclusion of the investigation.

Third, section 2511(2)(i)(III) requires that the person acting under color of law have reasonable grounds to believe that the contents of the communication to be intercepted will be relevant to the ongoing investigation. Fourth, section 2511(2)(i)(IV) requires that investigators intercept only the communications sent or received by trespassers. Thus, this section would only apply where the configuration of the computer system allows the interception of communications to and from the trespasser, and not the interception of non-consenting users authorized to use the computer.

Finally, section 217 of the Act amends section 2510 of title 18 to create a definition of "computer trespasser." Such trespassers include any person who accesses a protected computer (as defined in section 1030 of title 18) without authorization. In addition, the definition explicitly excludes any person "known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator for access to all or part of the computer." 18 U.S.C. § 2510(21). For example, certain Internet service providers do not allow their customers to send bulk unsolicited e-mails (or "spam"). Customers who send spam would be in violation of the provider's terms of service, but would not qualify as trespassers – both because they are authorized users and because they have an existing contractual relationship with the provider. These provisions will sunset December 31, 2005.

"While the act was primarily designed to increase federal law enforcement's abilities to investigate and prosecute terrorist organizations operating within the United States, the act also implemented sweeping changes which impact computer crime related investigations."

A publication of the DCIS Northeast Field Office

Defense Criminal Investigative Service
Northeast Field Office
10 Industrial Highway, Bldg. G, Mail Stop 75
Lester, PA 19113

Phone: (610) 595-1900
Fax: (610) 595-1934

Send comments to: Jives@dodig.osd.mil

We're on the Web!
www.dodig.osd.mil/dcis/dcismain.html

The Defense Criminal Investigative Service

"Protecting America's Warfighters"

The Defense Criminal Investigative Service is the investigative arm of the U.S. Department of Defense, Office of the Inspector General. As such, DCIS investigates criminal, civil, and administrative violations impacting the Defense Department. Typically, DCIS investigations focus upon computer crime involving U.S. military and civilian DoD systems, contract procurement fraud, bribery and corruption, health care fraud, anti-trust investigations, significant thefts of government property, export enforcement violations, environmental violations, and other issues that impact the integrity and effectiveness of the U.S. Department of Defense.

If you encounter issues that impact the U.S. Department of Defense, please call the DCIS office within your region.

DCIS Northeast Field Office.
10 Industrial Hwy., Bldg. G
Lester, PA 19113
Phone: (610) 595-1900
Fax: (610) 595-1934

DCIS Boston Resident Agency
Rm. 327, 495 Summer Street
Boston, MA 02210
Phone: (617) 753-3044
Fax: (617) 753-4284

DCIS Hartford Resident Agency
525 Brook Street, Suite 205
Rocky Hill, CT 06067
Phone: (860) 721-7751
Fax: (860) 721-6327

DCIS New Jersey Resident Agency
Wick Plaza 1, 100 Dey Pl., Ste. 102
Edison, NJ 08817
Phone: (732) 819-8455
Fax: (732) 819-9430

DCIS New York Resident Agency
One Huntington Quad, Suite 2C01
Melville, NY 11747
Phone: (516) 420-4302
Fax: (516) 420-4316

DCIS Pittsburgh Post of Duty
1000 Liberty Ave., Ste. 1310
Pittsburgh, PA 15222
Phone: (412) 395-6931
Fax: (412) 395-4557

DCIS Syracuse Resident Agency
441 S. Selina St., Ste. 304
Syracuse, NY 13202
Phone: (315) 423-5019
Fax: (315) 423-5099